Berner Fachhochschule
Technik und Informatik / RISIS

Neue E-Voting Systeme – Transparenz statt Geheimhaltung

Eric Dubuis, Stephan Fischli

Gefahren bei Internetwahlen (1)

SUISSE MONDE SPORTS FAITS DIVERS PEOPLE LOISIRS SOCIÉTÉ ÉCONOMIE A

Web Hard-/Software Jeux Images

Un citoyen a pu voter deux fois

INTERNET — Le système de vote électronique a permis à un électeur de voter à double ce week-end. La Chancellerie fédérale se veut rassurante, mais pour le Parti pirate, ce couac décrédibilise l'e-voting.

Par Simon Koch. Mis à jour le 12.03.2012
33 Commentaires

Recommander 9

Gefahren bei Internetwahlen (2)

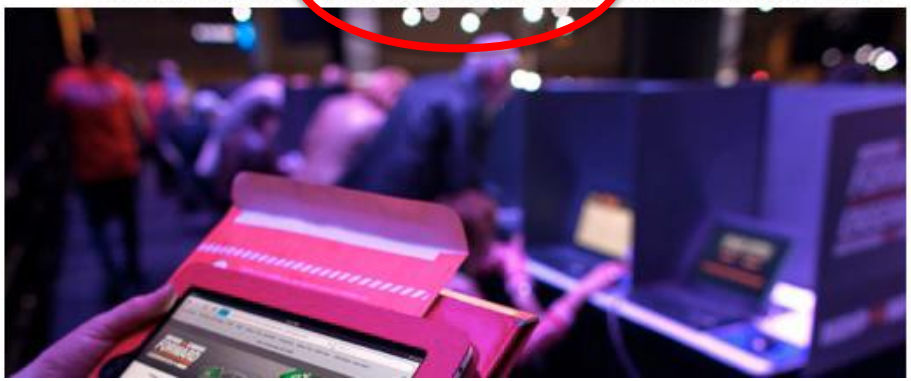
NATIONAL POST

News | Canada | Graphics | World

NEWS

Cyber attack on NDP leadership vote involved more than 10,000 computers

National Post Staff | Mar 27, 2012 12:07 PM ET | Last Updated: Mar 27, 2012 1:44 PM ET



Gefahren bei Internetwahlen (3)

L'INFORMATICIEN

ACTUALITÉS DÉBATS DOSSI

TECHNOS RÉSEAU MOBILITÉ SÉCURITÉ SERVEURS CLOUD HPC LOGICIEL DÉVELOPPEMENT EMPLOI

Législatives : 130 000 Français ont voté dangereusement par Internet

par Emilien Ercolani, le 30 mai 2012 11:57

Les Français de l'étranger, qui peuvent voter par Internet depuis le 23 mai, ont été potentiellement la cible de détournements de leurs votes. Malgré la dénonciation d'une possible faille lors du vote, rien ne semble avoir bougé.

Décidément, le vote autre que sur un morceau de papier a du mal à rassurer, et encore... Déjà en 2007, nous relayions dans un papier **les alertes des informaticiens** concernant le vote électronique (des machines dans les urnes). Aujourd'hui, c'est le vote par Internet qui est la cible de menaces. Et pour la première année, les Français de l'étranger avaient la possibilité d'utiliser ce moyen.

Sur le papier, la démarche est excellente, puisqu'elle évite de se déplacer dans des bureaux de vote. En revanche, la presse fait état de gros problèmes de sécurité qui d'une part n'ont pas été réglés, d'autre part ont été presque ignorés. Pourtant, dans un **document d'une vingtaine de pages** (ci-dessous) assorti d'une vidéo en situation réelle, le développeur Laurent Grégoire démontre par A + B comment il est possible de détourner un vote : vous votez pour monsieur X, et c'est finalement madame Y qui reçoit votre vote.

Une attaque relativement simple

Le document, intitulé « Comment mon ordinateur a voté à ma place (et à mon insu) », est très

Inhalt

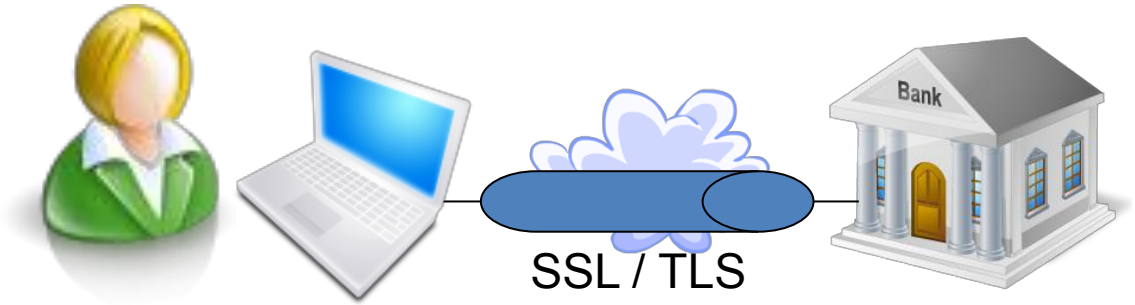
1. Einführung
2. Situation in der Schweiz
3. Anforderungen an E-Voting-Systeme
4. Konzept eines verifizierbaren E-Voting-Systems
5. Fazit und Ausblick

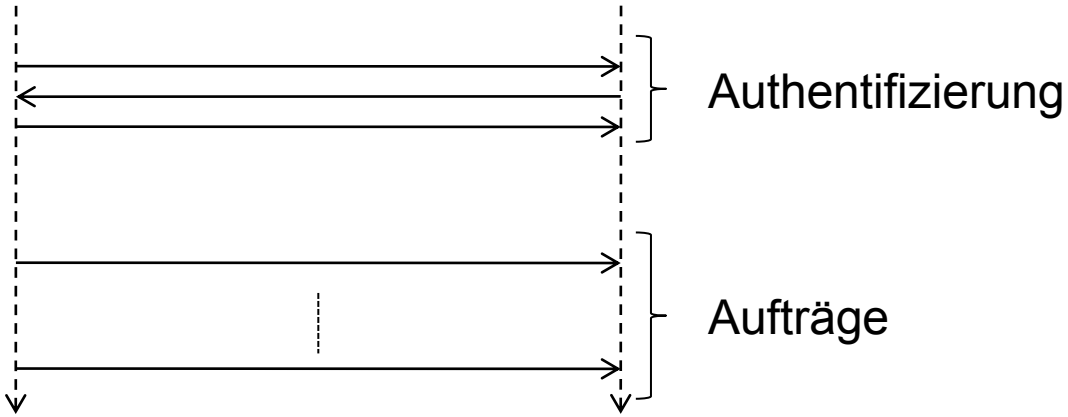
Inhalt

E-Banking – vereinfacht

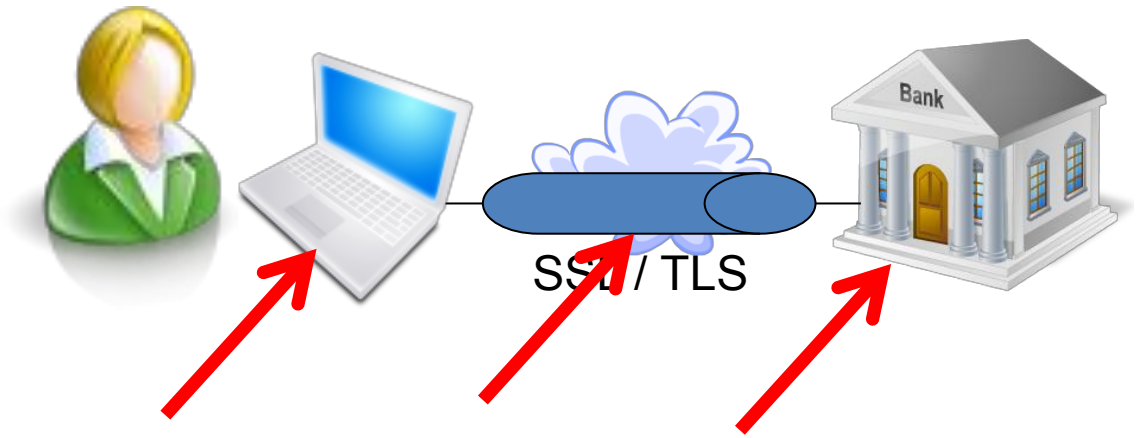
- Vertrag
- Bank kennt Kunde
- Dienste:
  - Bargeldbezug (Bancomat)
  - E-Banking (Internet)

E-Banking – Ablauf

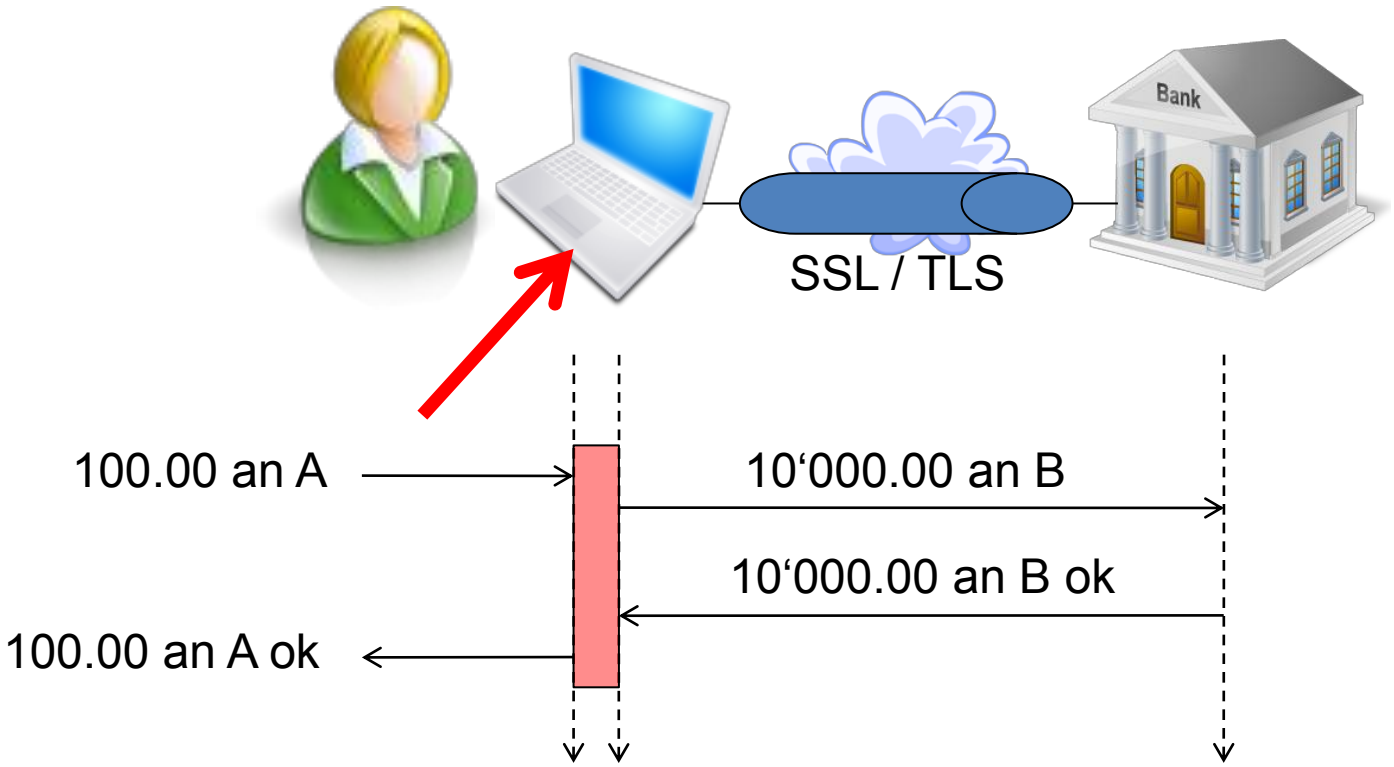




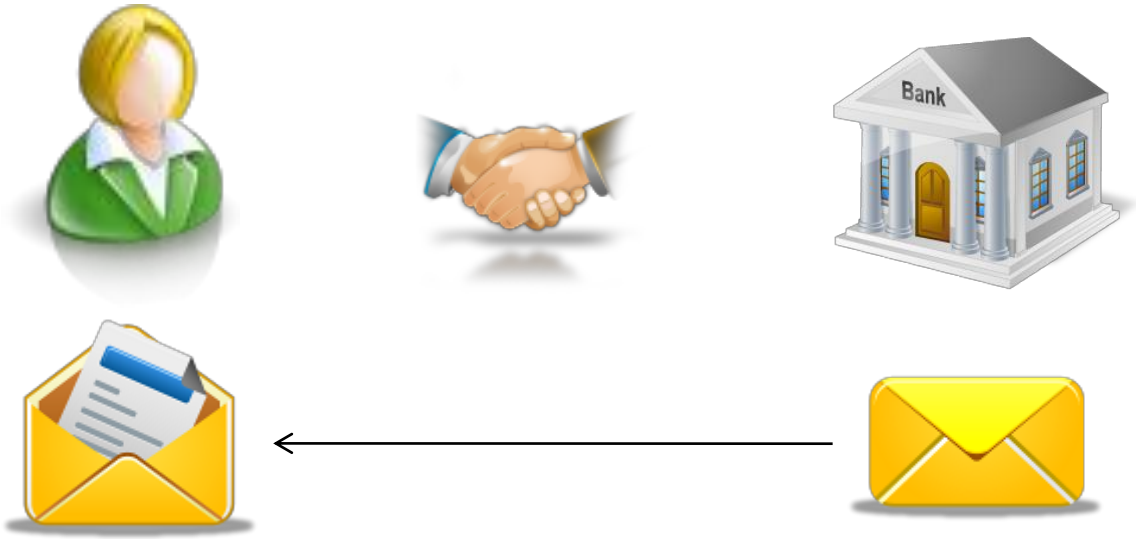
E-Banking – Angriffspunkte



E-Banking – Malware



E-Banking – Auszug

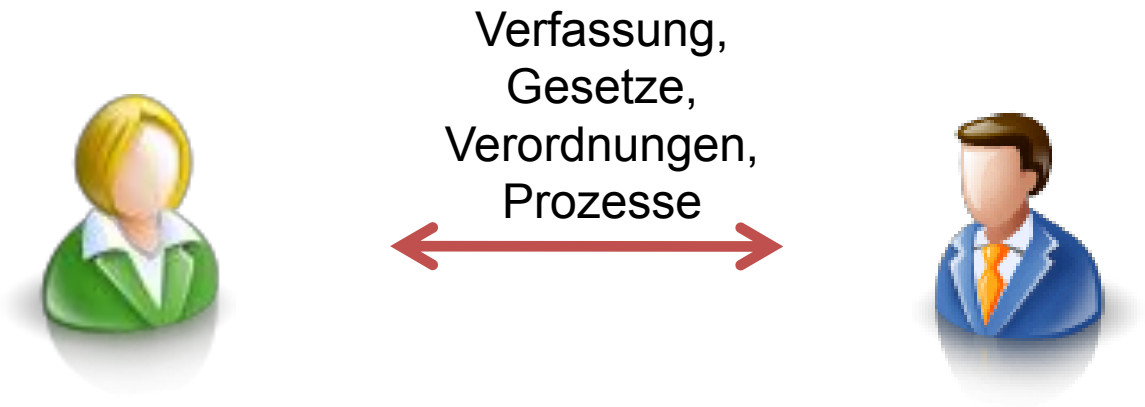


E-Banking – Fazit

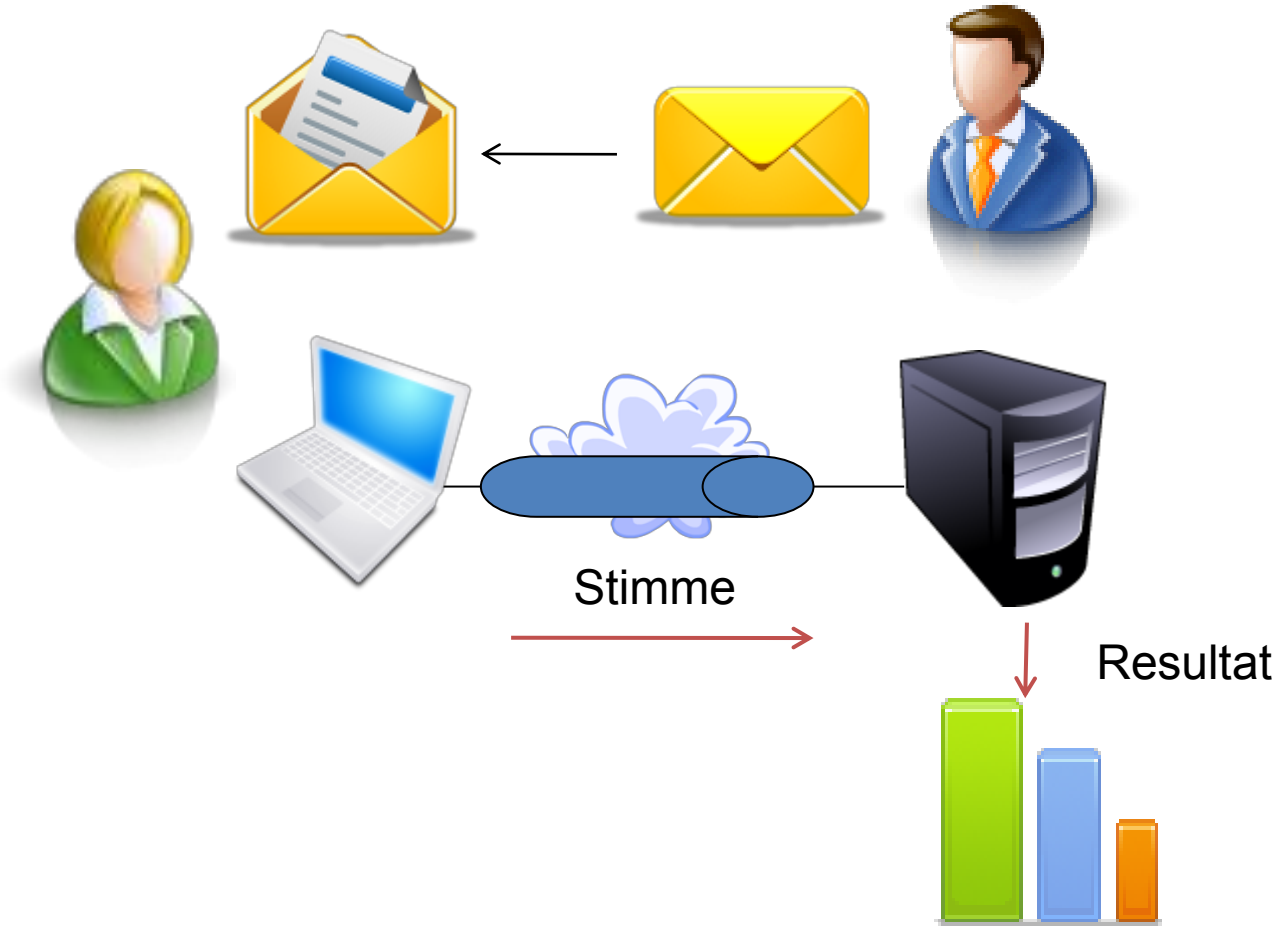
- Die Kundin / der Kunde merkt am Ende der Abrechnungsperiode, wenn etwas nicht stimmt

... und wie ist es bei E-Voting?

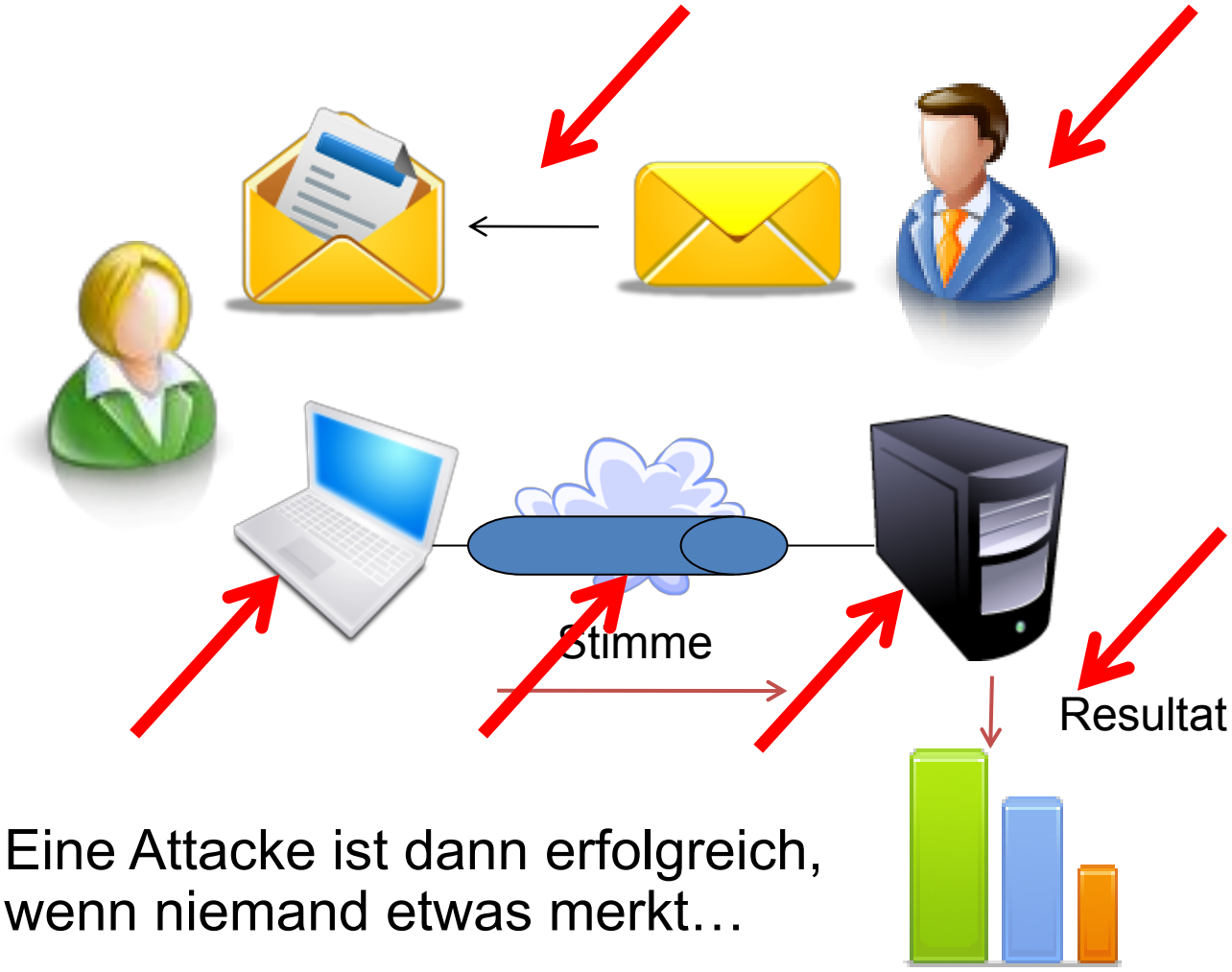
E-Voting – Bürger ↔ Verwaltung



E-Voting – vereinfacht



E-Voting – vereinfacht



Eine Attacke ist dann erfolgreich,
wenn niemand etwas merkt…

E-Voting – als „Black Box“-System

Fragen:

- Wurde meine Stimme gezählt?
- Wurde richtig gezählt?
- Wurden nur berechtigte Stimmen gezählt?

Inhalt

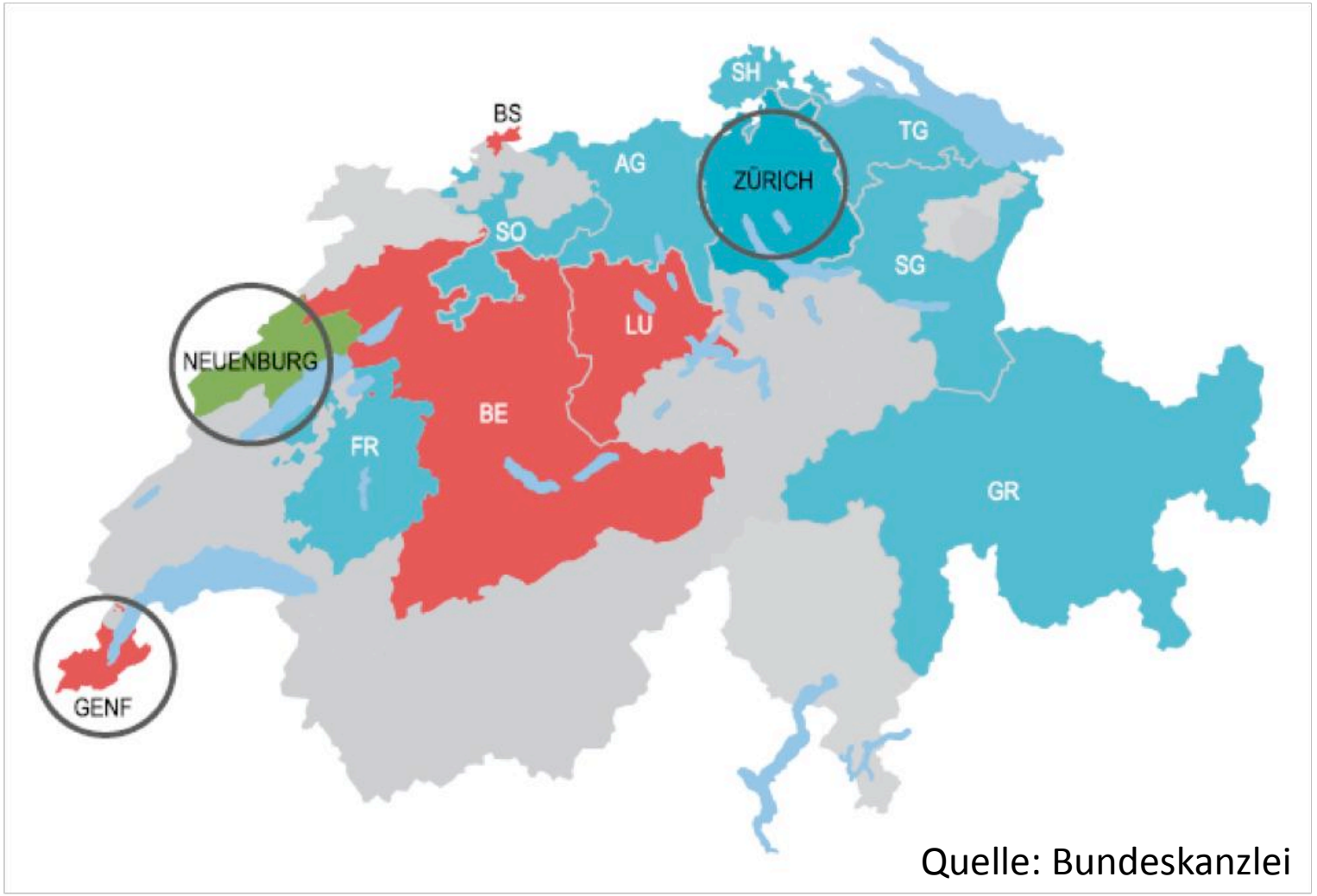
Warum braucht es E-Voting?

- Auslandschweizer (Gesetz)

Quelle: swissinfo.ch

- Höhere Wahlbeteiligung (Internet-Generation)
- Bessere Effizienz, geringere Kosten

E-Voting in der Schweiz (1)

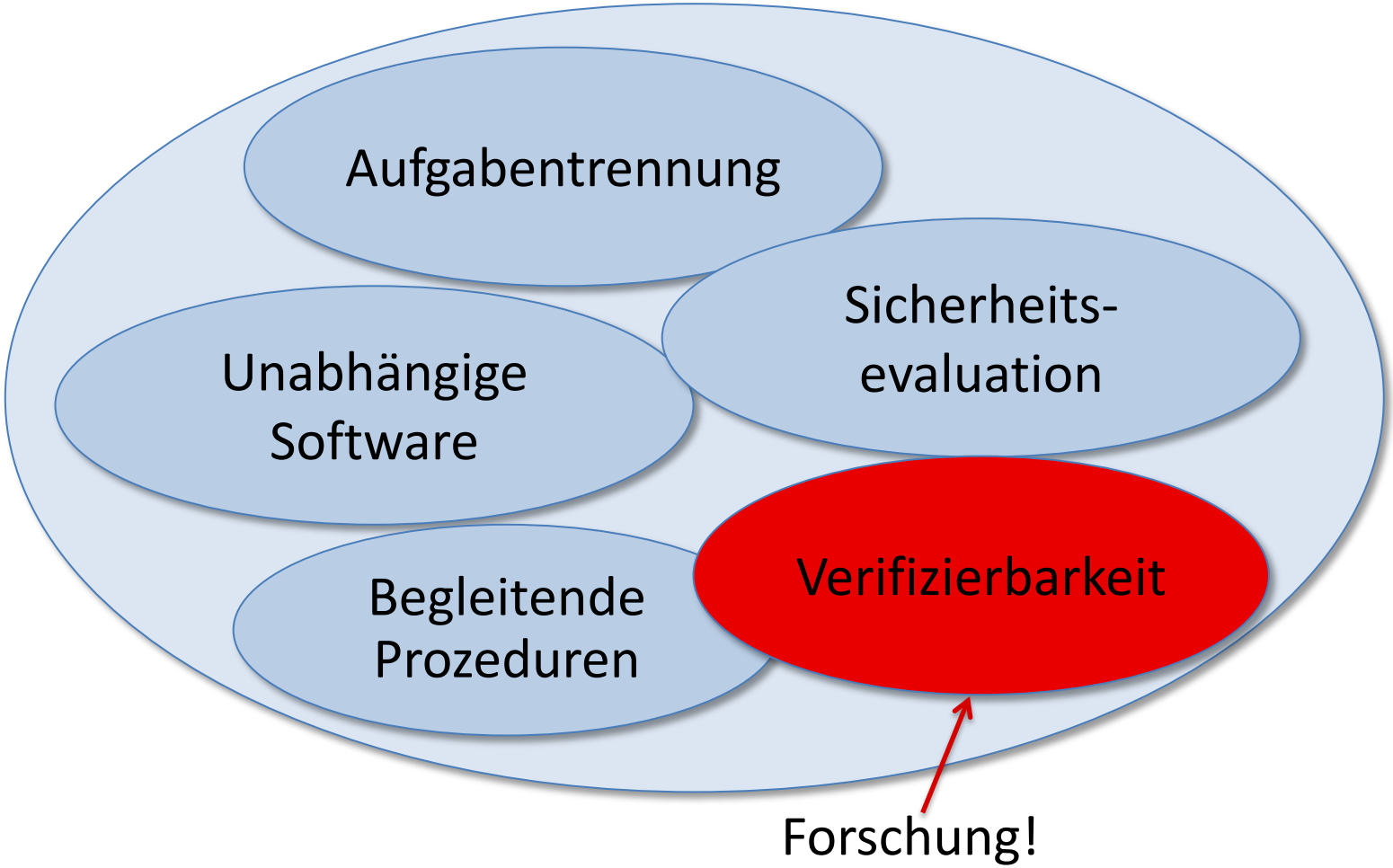


Quelle: Bundeskanzlei

E-Voting in der Schweiz (2)

- Drei kantonale Systeme
- Einsatz auf allen 3 politischen Ebenen
- Abstimmungen, Wahlen
- Rolle Bundeskanzlei (vote électronique)
  - koordiniert E-Voting-Aktivitäten
  - bewilligt den Einsatz von E-Voting-Systemen

Massnahmen zur Bildung von Vertrauen



E-Voting-Gruppe der BFH

- Berner Fachhochschule, Technik und Informatik
  Research Institute for Security in the Information Society (RISIS)
- Mitglieder
  - Eric Dubuis, Stephan Fischli, Rolf Haenni, Reto Koenig
  - 1 wissenschaftlicher Mitarbeiter, 1 Doktorand
  - 2 Master-Studenten
- Aktiv seit anfangs 2008
  - Swiss E-Voting Workshops
  - BK-Konzept, Projekte
  - Publikationen

Inhalt

1. Einführung
2. Situation in der Schweiz
3. Anforderungen an E-Voting-Systeme
4. Konzept eines verifizierbaren E-Voting-Systems
5. Fazit und Ausblick

Anforderungen beim E-Voting (1)

- Wahlberechtigung
  - Nur Wahlberechtigte, 1 Stimme pro Wahlberechtige(r)
    - Authentifizierung (wer?)
    - Autorisierung (stimmberechtigt / noch nicht gewählt?)
- Integrität
  - Stimmen können nicht geändert werden
  - Stimmen können nicht entfernt oder hinzugefügt werden
- Korrektheit
  - Alle gültigen Stimmen wurden im Resultat berücksichtigt
- Wahlgeheimnis
  - Stimme ist geheim

Anforderungen beim E-Voting (2)

- Anonymität
  - Kein Rückschluss auf die einzelnen Wähler
- Gerechtigkeit
  - Keine Teilresultate vor Urnenschluss
- Individuelle Verifizierbarkeit
  - Stimme richtig erfasst und gezählt
- Universelle Verifizierbarkeit
  - Alle Stimmen richtig erfasst und gezählt

Nicht-fachliche Anforderungen

- Verfügbarkeit/Robustheit des Systems
- Sicherheit trotz unsicheren Client-Plattformen
- Effizienz der Stimmabgabe und Resultatermittlung
- Benutzerfreundlichkeit und Barrierefreiheit

... und diese machen die Sache nicht leichter!

Inhalt

Herausforderung

Entwicklung eines E-Voting-Systems mit teilweise widersprüchlichen Anforderungen:

- Verifizierbarkeit $\leftrightarrow$ Wahlgeheimnis
- Anonymität $\leftrightarrow$ Wahlberechtigung

Kryptografische Zutaten

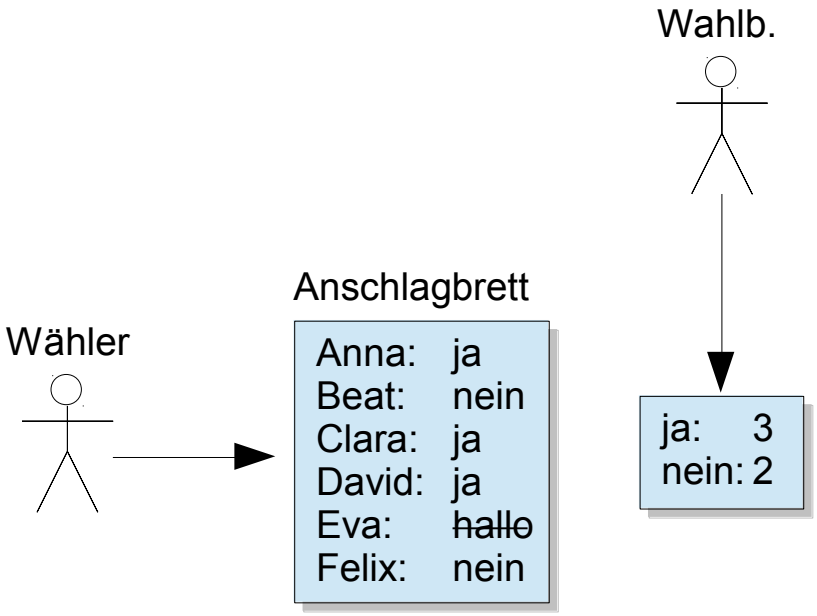
- Schlüssel und Zertifikate (PKI)
- Digitale Signaturen
- Asymmetrische Verschlüsselung
- Mix-Netzwerke
- Zero-Knowledge-Beweise
- Threshold-Systeme
- Blinde Signaturen
- Anonyme Kanäle
- Homomorphe Auszählung

Inhalt

1. Einführung
2. Situation in der Schweiz
3. Anforderungen an E-Voting-Systeme
4. Konzept eines verifizierbaren E-Voting-Systems
   - Idee des Anschlagbretts
   - Protokollbeschreibung
5. Fazit und Ausblick

Idee des Anschlagbretts (1)

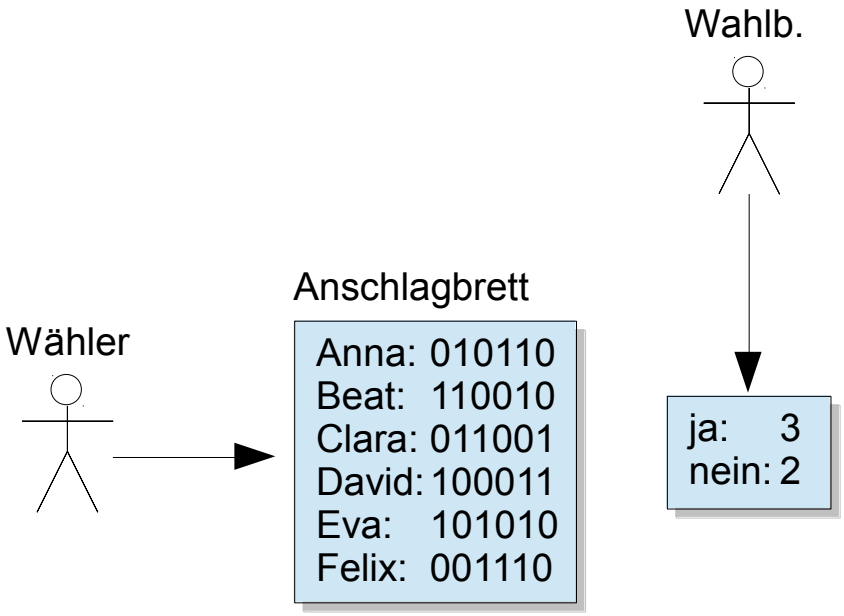
Wählende veröffentlichen ihre Stimmen mit ihrem Namen



✓ Ind. Verifizierbarkeit
✓ Univ. Verifizierbarkeit
✗ Wahlgeheimnis
✗ Anonymität
✓ Authentifizierung
✗ Autorisierung
✓ Integrität
✓ Korrektheit
✗ Gerechtigkeit
✗ Quittungsfreiheit

Idee des Anschlagbretts (2)

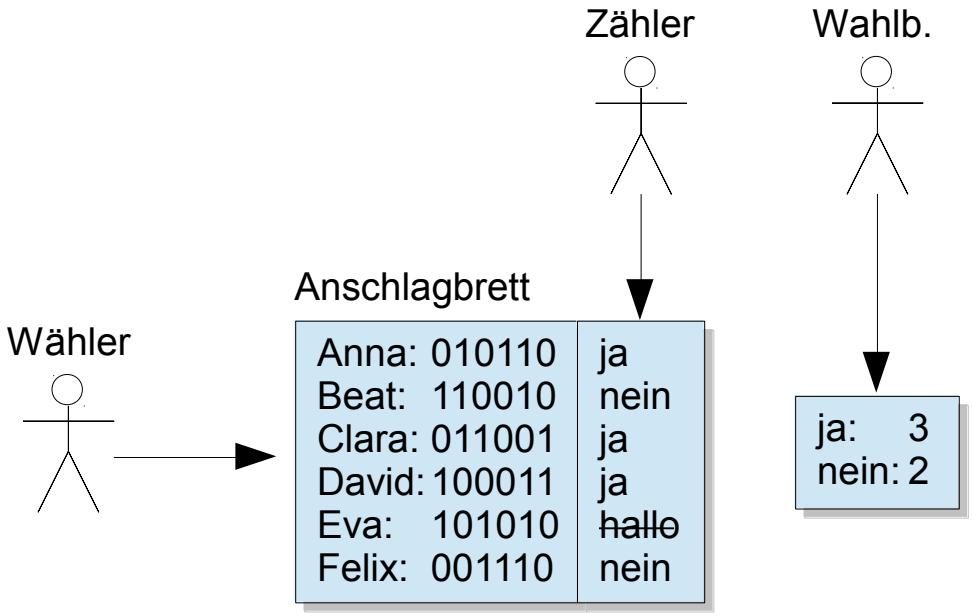
Wählende verschlüsseln ihre Stimmen



✓Ind. Verifizierbarkeit ✗Univ. Verifizierbarkeit
✓Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✗Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

Idee des Anschlagbretts (3)

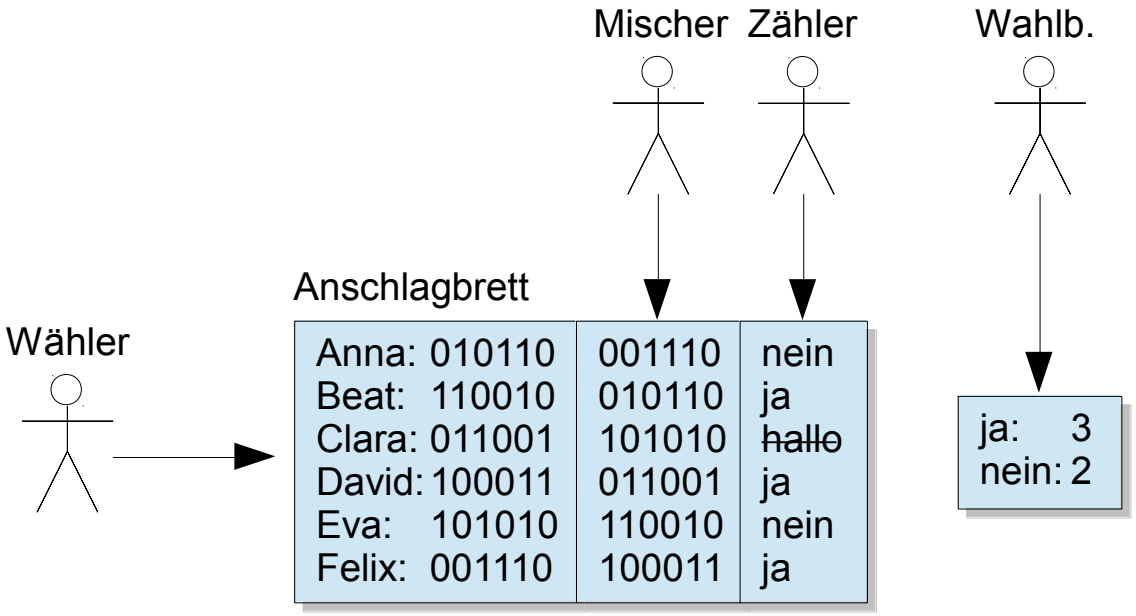
Zähler entschlüsselt Stimmen



✓Ind. Verifizierbarkeit ✓Univ. Verifizierbarkeit
✗Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✓Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

Idee des Anschlagbretts (4)

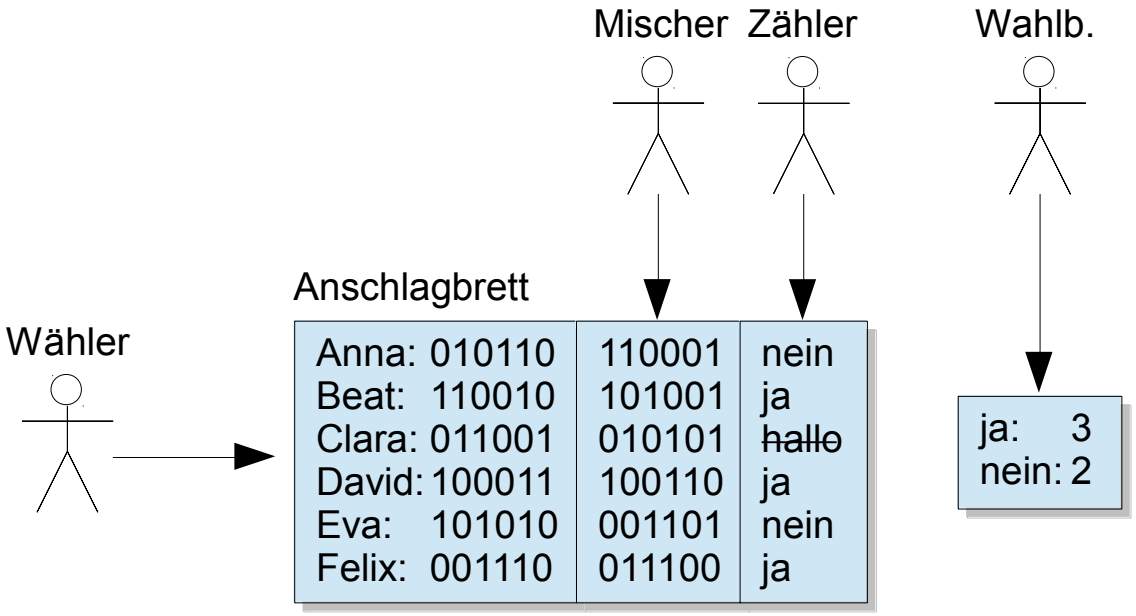
Verschlüsselte Stimmen werden gemischt



✓ Ind. Verifizierbarkeit
✓ Univ. Verifizierbarkeit
✗ Wahlgeheimnis
✗ Anonymität
✓ Authentifizierung
✗ Autorisierung
✓ Integrität
✓ Korrektheit
✓ Gerechtigkeit
✗ Quittungsfreiheit

Idee des Anschlagbretts (5)

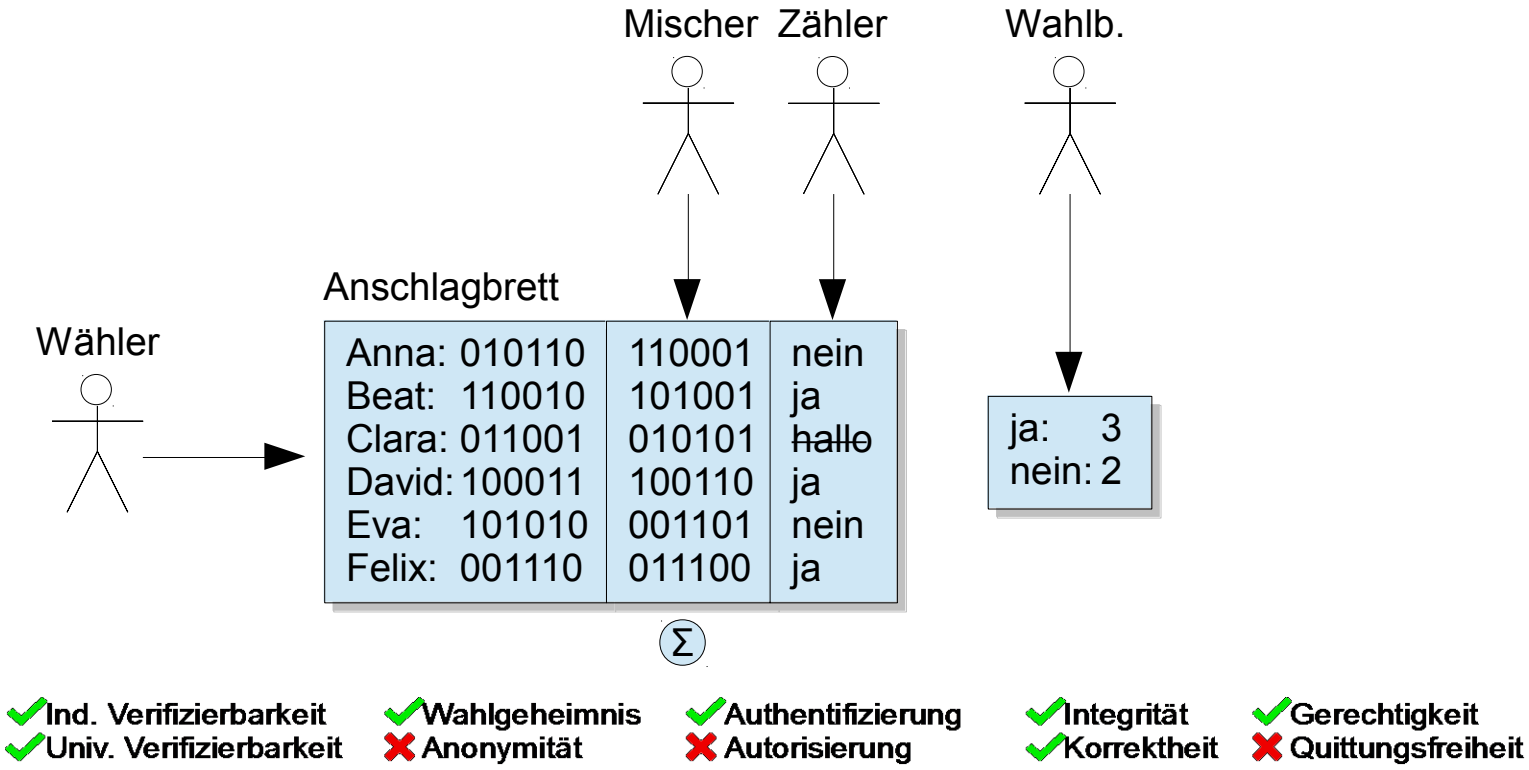
Verschlüsselte Stimmen werden kryptografisch gemischt



✓Ind. Verifizierbarkeit ✗Univ. Verifizierbarkeit
✓Wahlgeheimnis ✗Anonymität
✓Authentifizierung ✗Autorisierung
✓Integrität ✗Korrektheit
✓Gerechtigkeit ✗Quittungsfreiheit

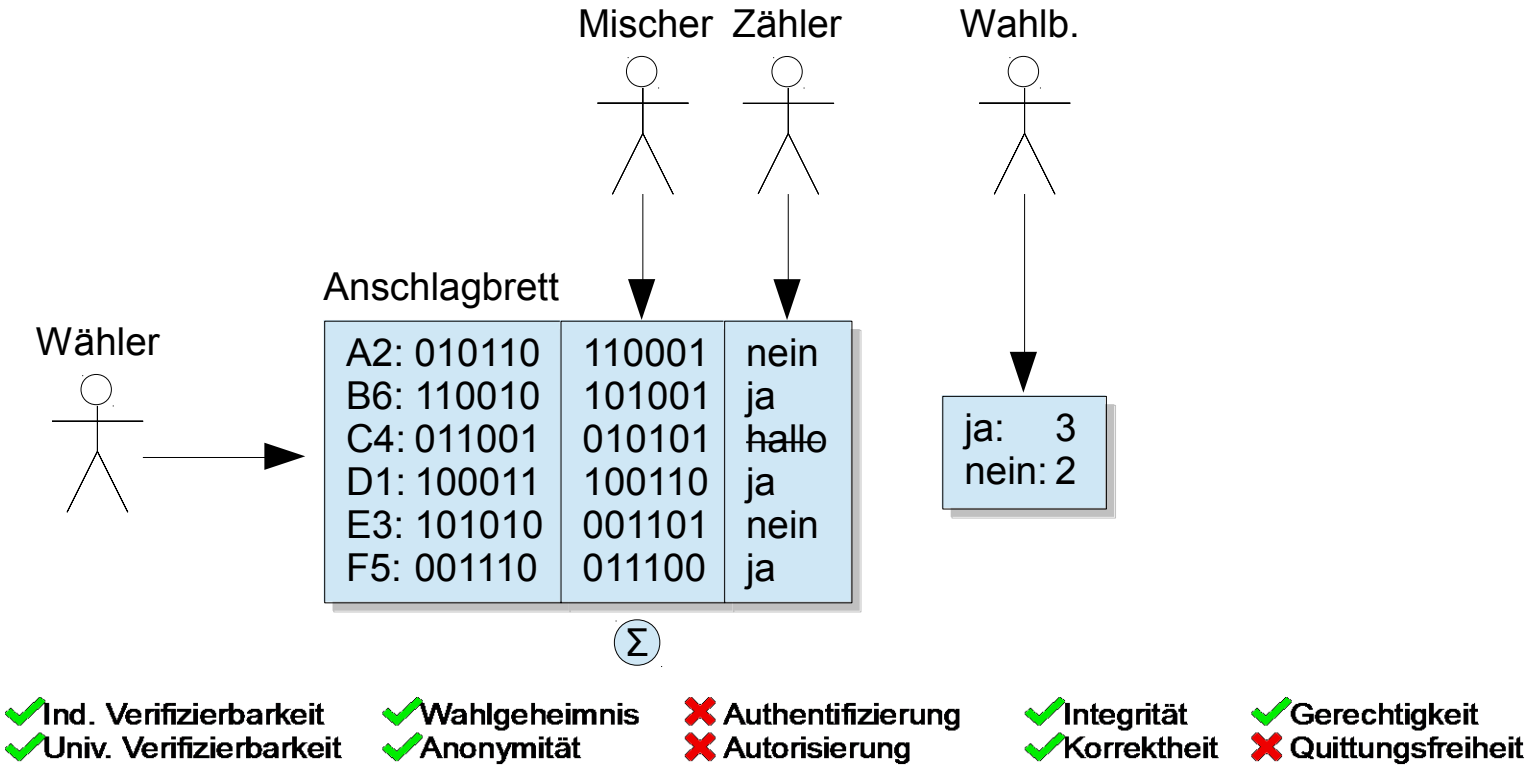
Idee des Anschlagbretts (6)

Mischer beweist die Korrektheit des Mischens



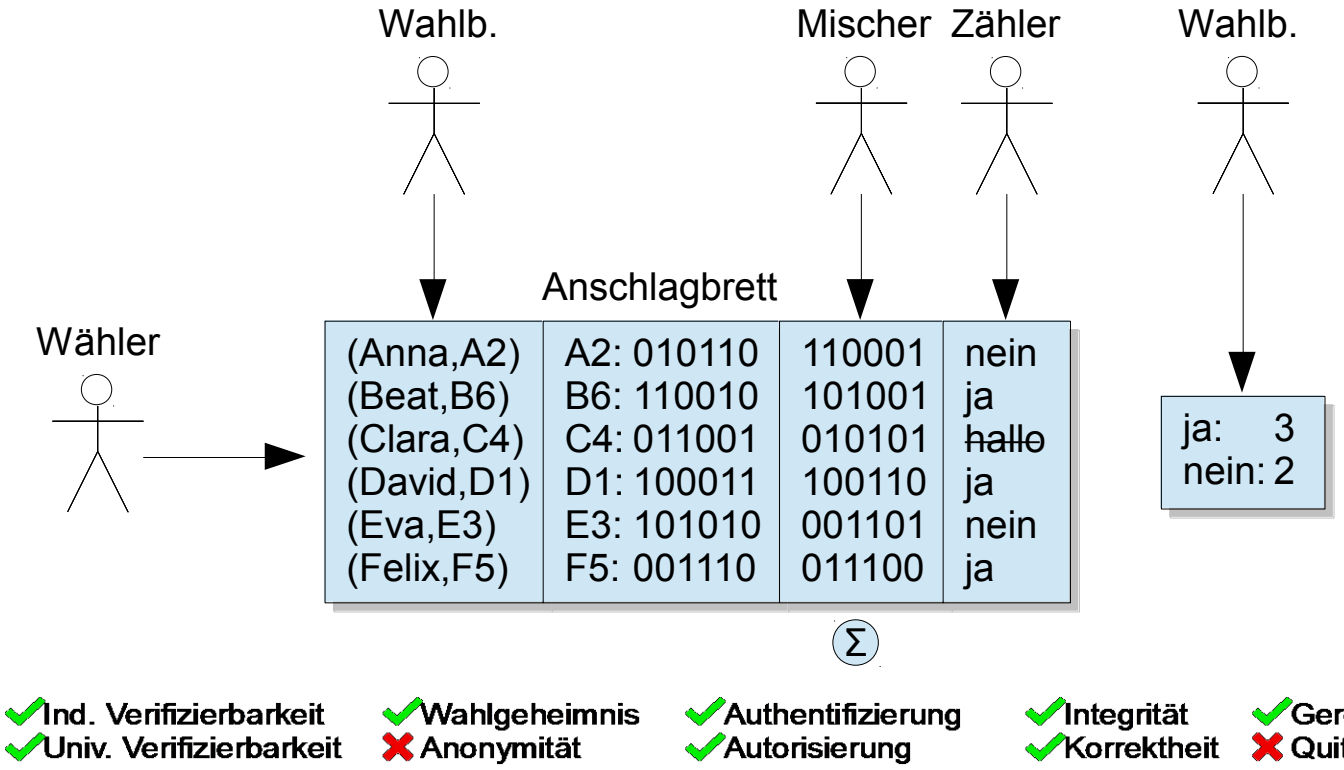
Idee des Anschlagbretts (7)

Wählende stimmen mit einem Pseudonym ab



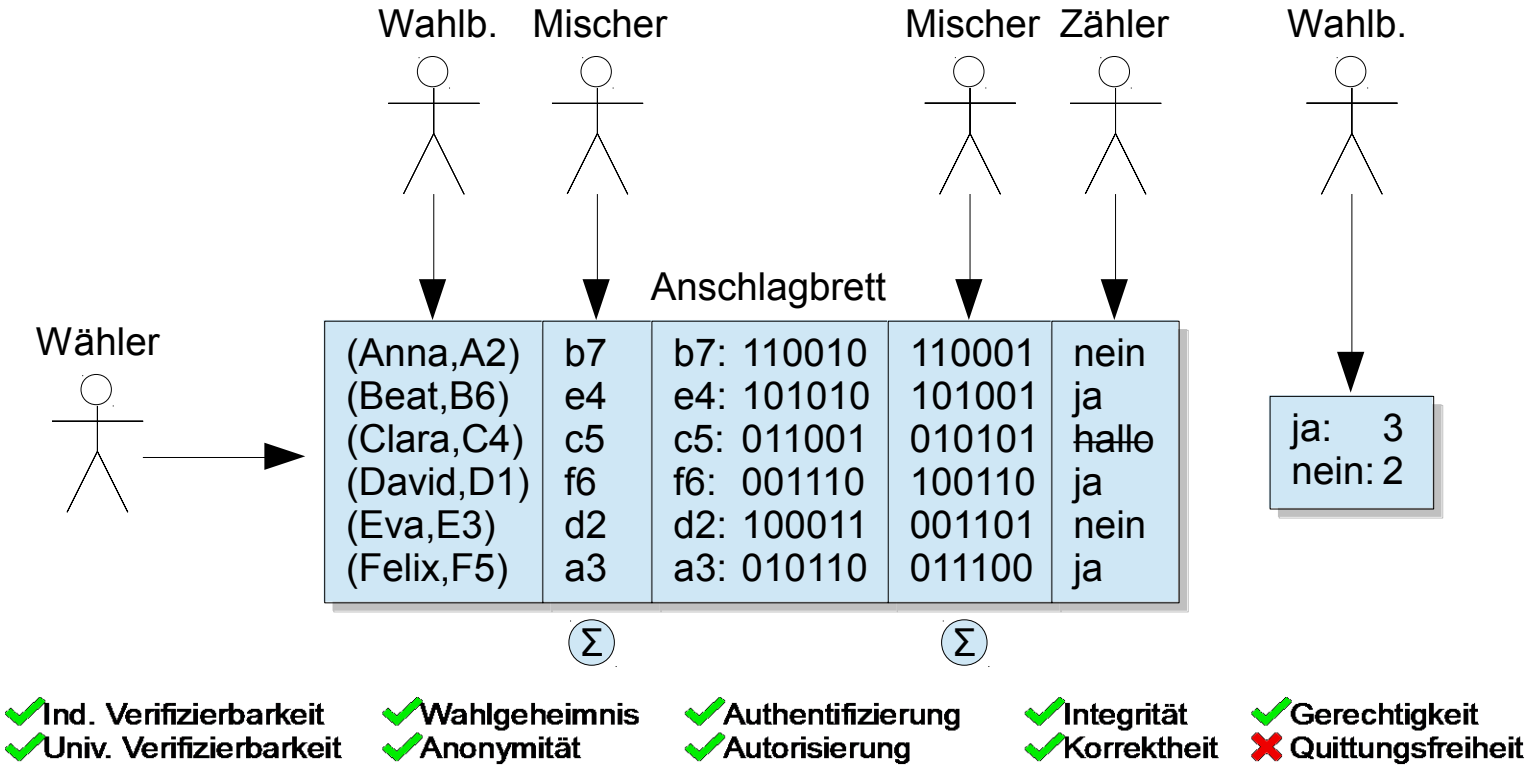
Idee des Anschlagbretts (8)

Pseudonyme werden von der Wahlbehörde zertifiziert



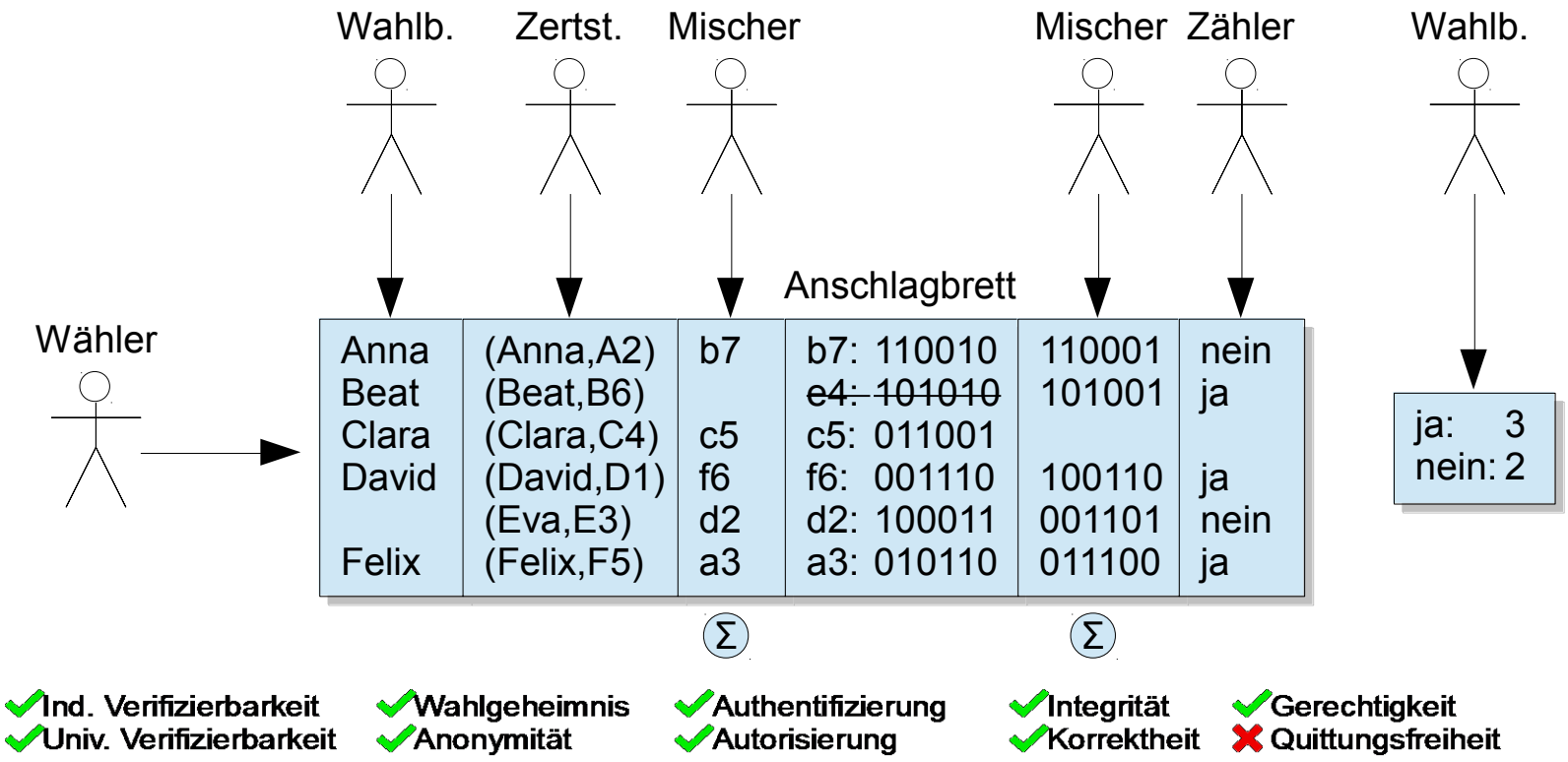
Idee des Anschlagbretts (9)

Pseudonyme werden kryptografisch gemischt



Idee des Anschlagbretts (10)

Wahlbehörde veröffentlicht Wählerverzeichnis



Inhalt

1. Einführung
2. Situation in der Schweiz
3. Anforderungen an E-Voting-Systeme
4. Konzept eines transparenten E-Voting-Systems
   - Idee des Anschlagbretts
   - Protokollbeschreibung
5. Fazit und Ausblick

Protokoll: Akteure

Zertifizierung

Wahlbehörde

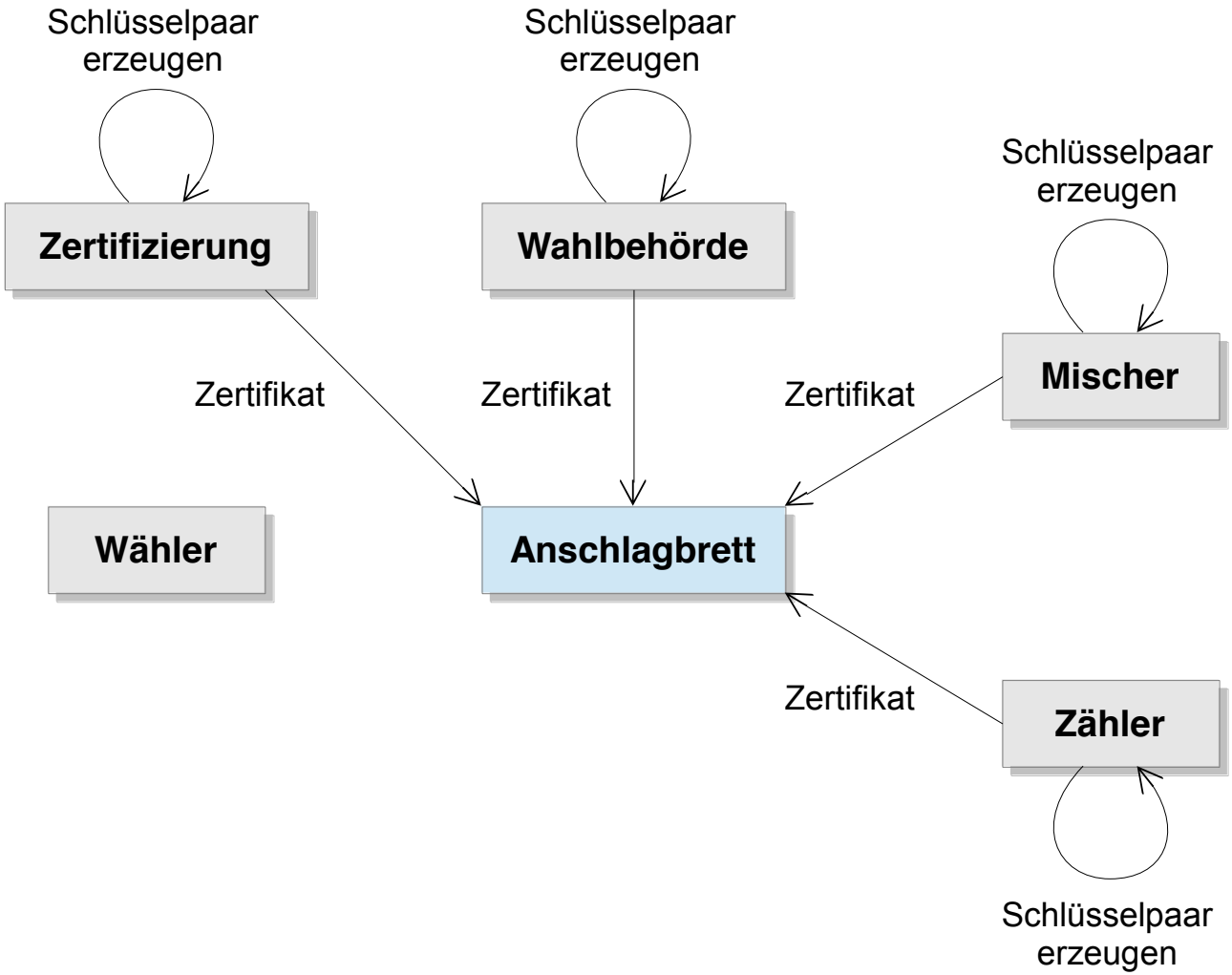
Mischer

Wähler

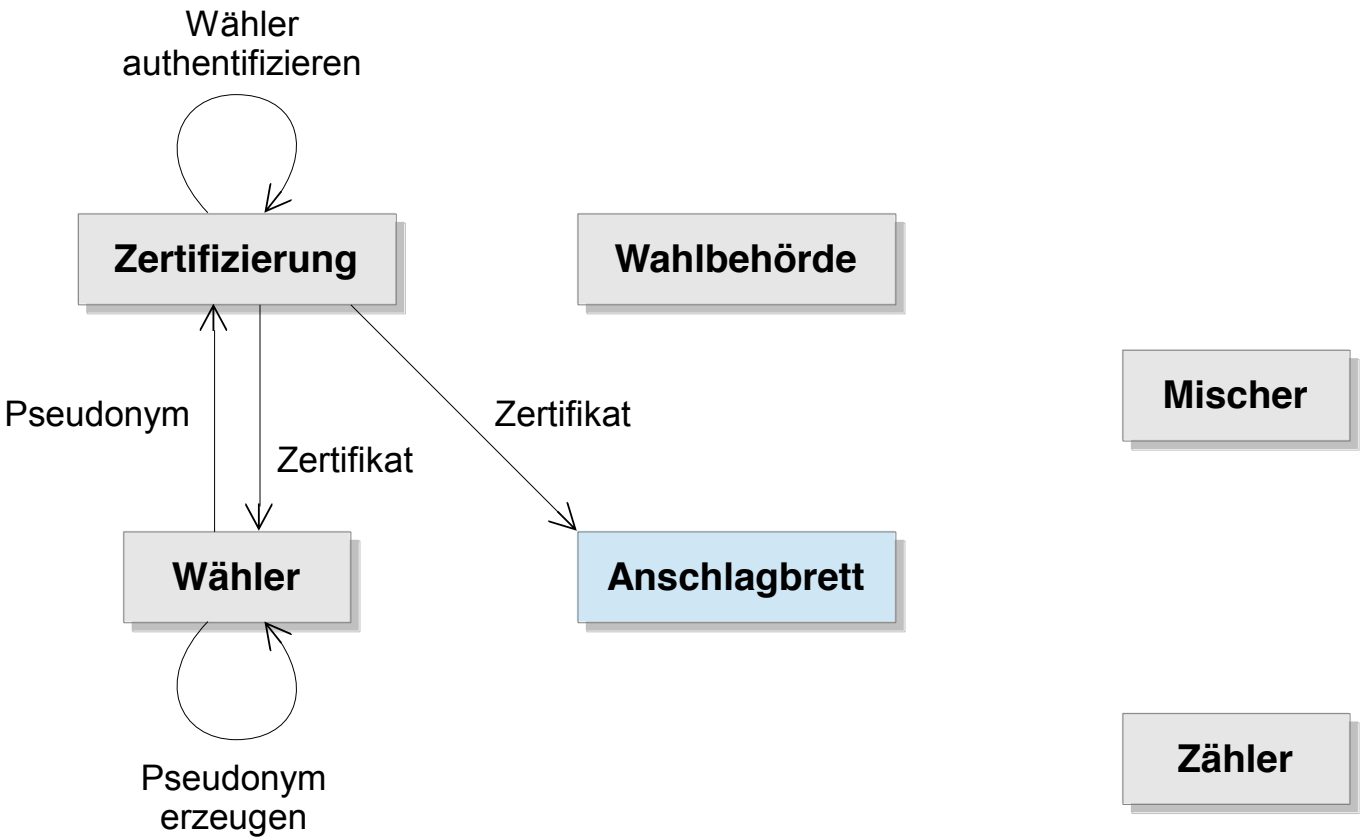
Anschlagbrett

Zähler

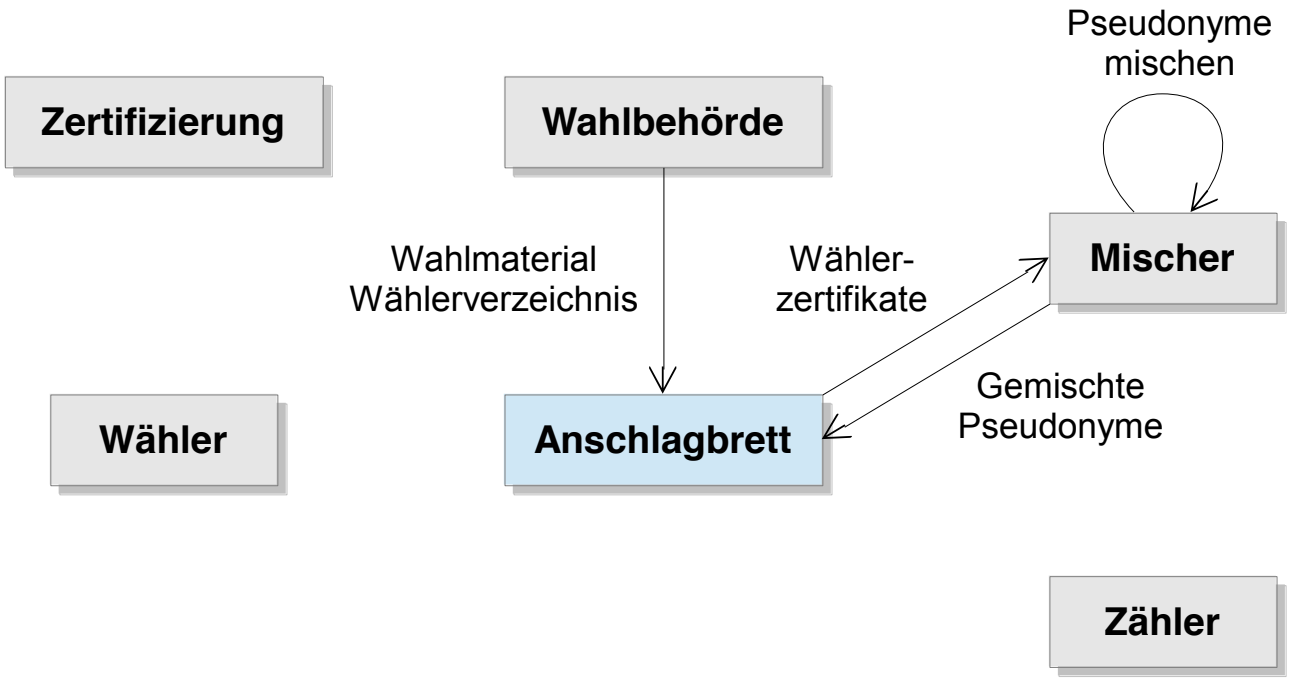
Protokoll: Setup



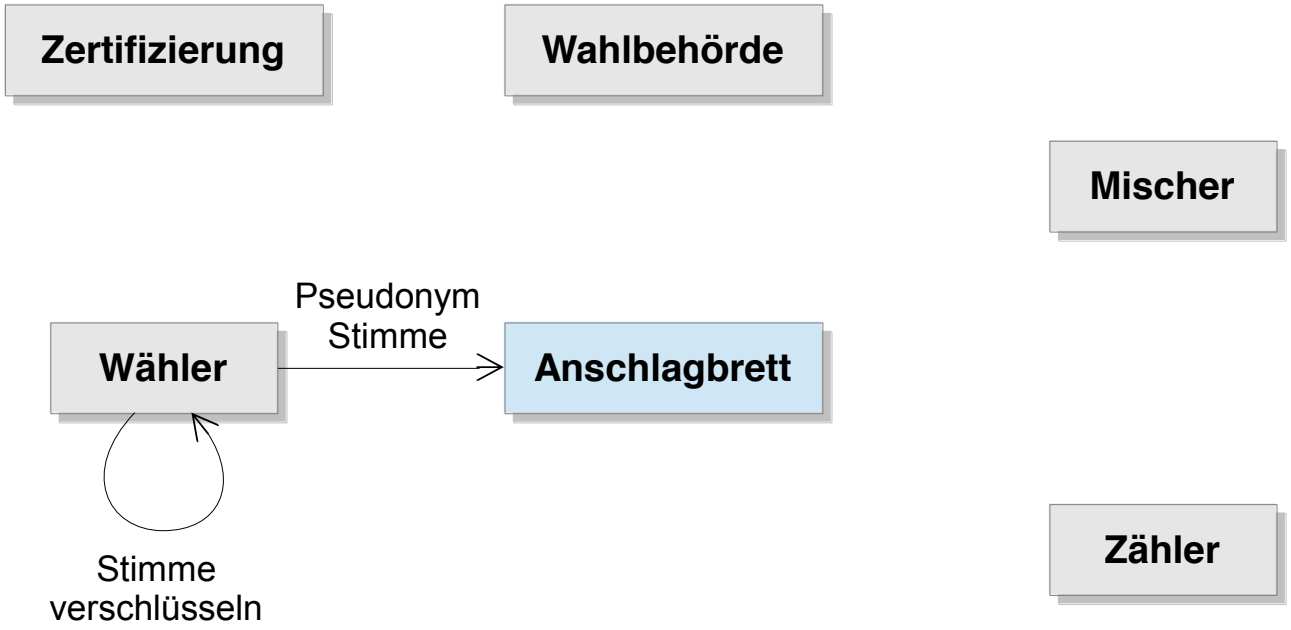
Protokoll: Registrierung



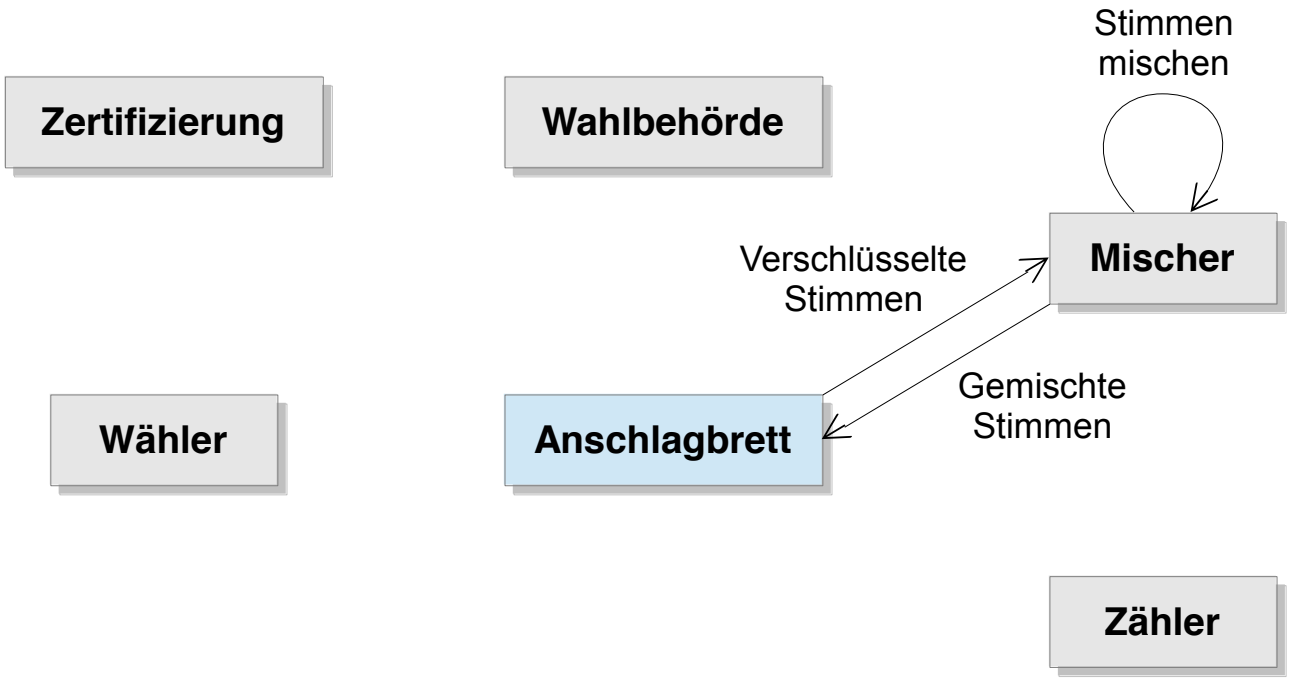
Protokoll: Wahlvorbereitung



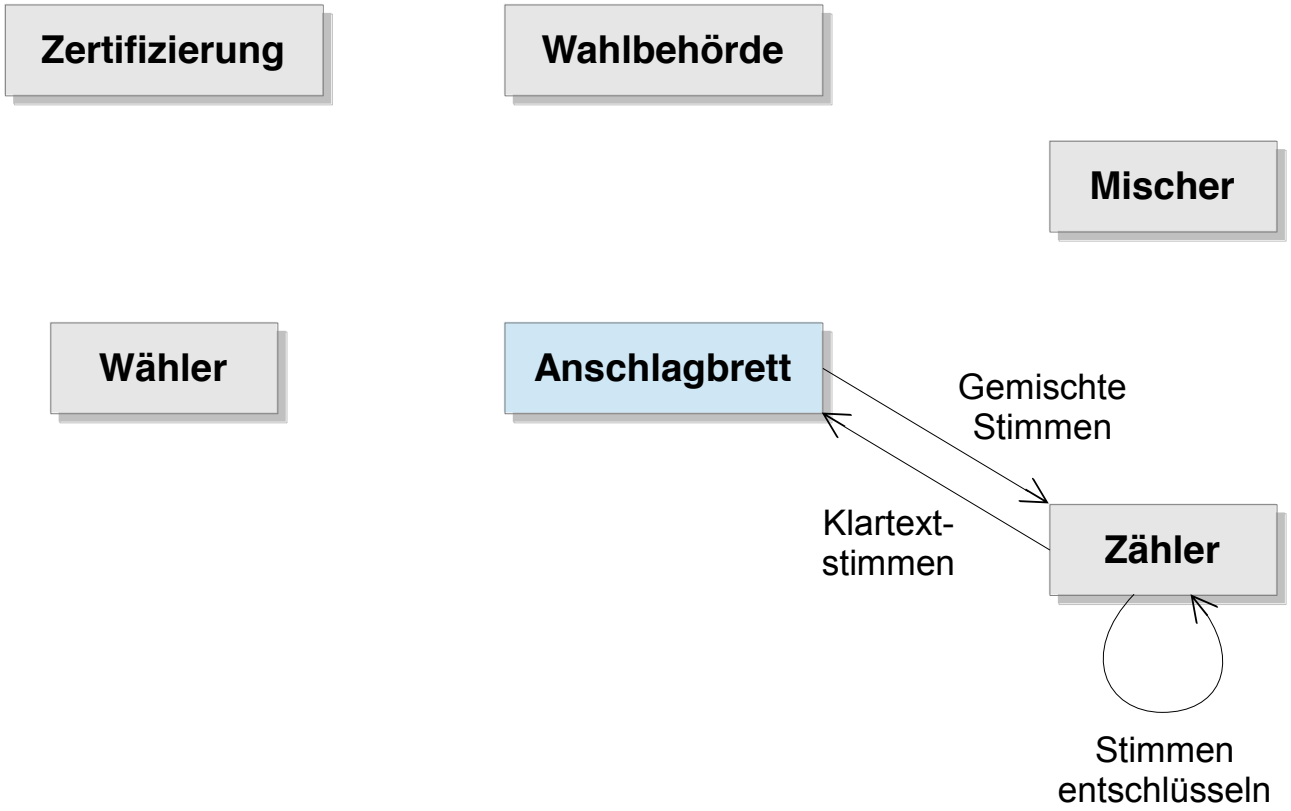
Protokoll: Stimmabgabe



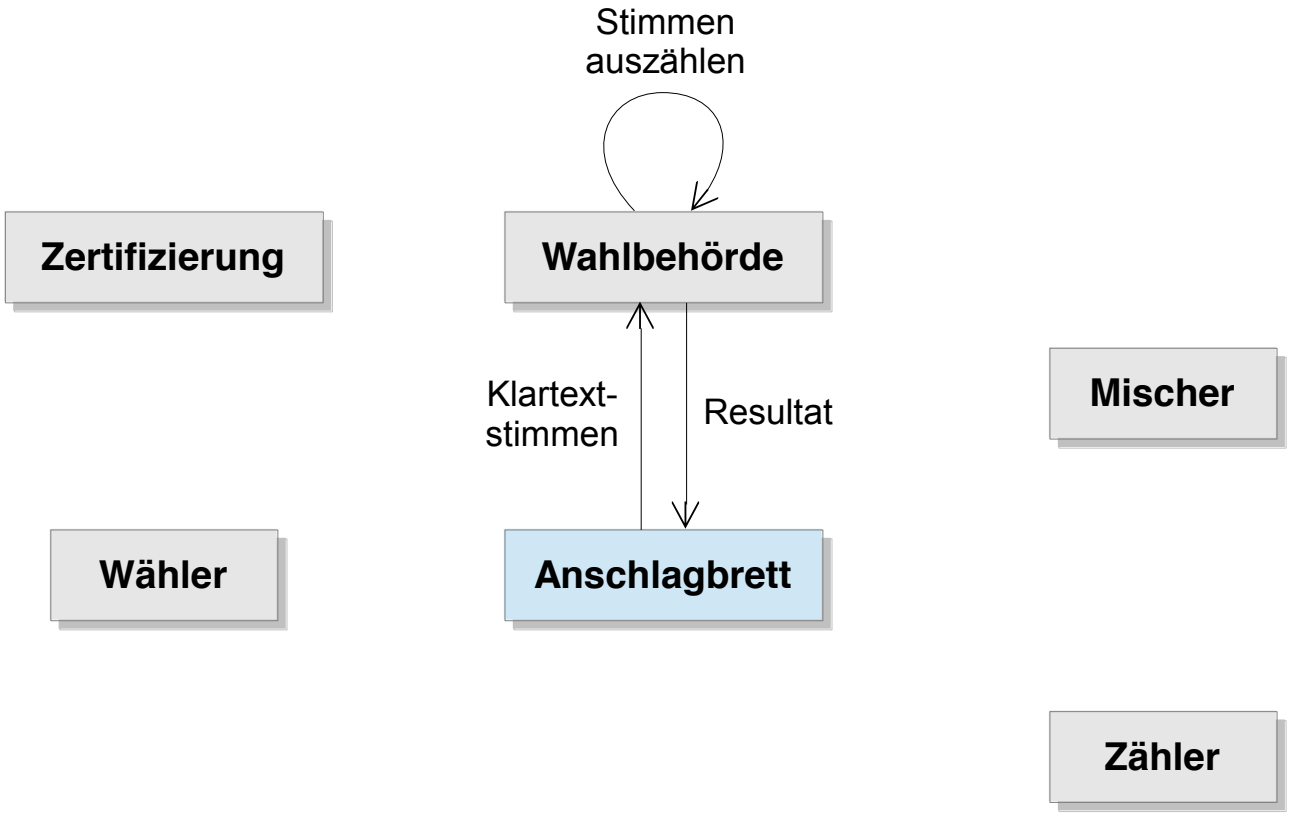
Protokoll: Wahlnachbereitung (1)



Protokoll: Wahlnachbereitung (2)



Protokoll: Auszählung



Et voilà!

Inhalt

1. Einführung
2. Situation in der Schweiz
3. Anforderungen an E-Voting-Systeme
4. Konzept eines verifizierbaren E-Voting-Systems
5. Fazit und Ausblick

Fazit

Ergebnis:

- Die meisten der Anforderungen sind erfüllt

Offene Probleme:

- Anschlagbrett versus Langzeitsicherheit
- Anschlagbrett versus Nötigung
  → Italian Attack
- Problem der unsicheren Plattform
  → Wahlgerät mit Wahlkarte

UniVote-Projekt als „Proof of Concept“

- Umfeld
  - Universitäten Bern und Zürich, BFH
  - Studentenratswahlen
- Anforderungen
  - Authentifizierung über SWITCHaai
  - keine vorgängige Registrierung
  - Datenschutz
- Protokolländerungen gegenüber Konzept
  - Wählerinnen / Wähler können sich auch erst während des Wahlvorgangs registrieren

Roadmap der Bundeskanzlei

- Schrittweiser Ausbau (Strategische Planung 2011)
  - Erhöhung der Limiten:
    aktuell 10% Schweiz; 20% Kantone bei Ständemehr
- Dritter Bericht zuhanden des Bundesrats

Kontakt

RISIS
http://ti.bfh.ch/risis

E-Voting-Gruppe
http://e-voting.bfh.ch

Dr. Eric Dubuis
eric.dubuis@bfh.ch

Dr. Rolf Haenni
rolf.haenni@bfh.ch

Dr. Stephan Fischli
stephan.fischli@bfh.ch